IDOT PTC
Safety Program Overview

W. Klinck

28 March, 2001

IDOT PTC Safety Topics

- System Requirements
- Safety Critical System Development
- Hazard And Risk Analyses
- UVA Effort
- Safety Concepts Overview
- Formal Documentation
- Verification, Validation And Testing
- Product Safety Plan (PSP)
- Approval
- Near Term Action

System Requirements

- **Safety Requirements Sources**
  - **System Spec Version 3.1**
    - **20 Safety Requirements In Paragraphs 4.11.1 And 4.11.2**
  - **Railroad Safety Program Plan**
    - **Generated for IDOT PTC as required by RSAC Draft Rule #8**
    - **Based Upon IEEE P1483 And MIL-STD-882C**
  - **RSAC Draft Rule #8**
    - **Currently Under Public Review**
  - **Derived Requirements From Safety Analyses**
- **System Spec V3.1 objectives**
  - **Use COTS hardware and software**
  - **Handle authorities and enforcements in a Vital manner**
  - **Safety analyses based upon the emerging Processor Based Rule (NPRM)**

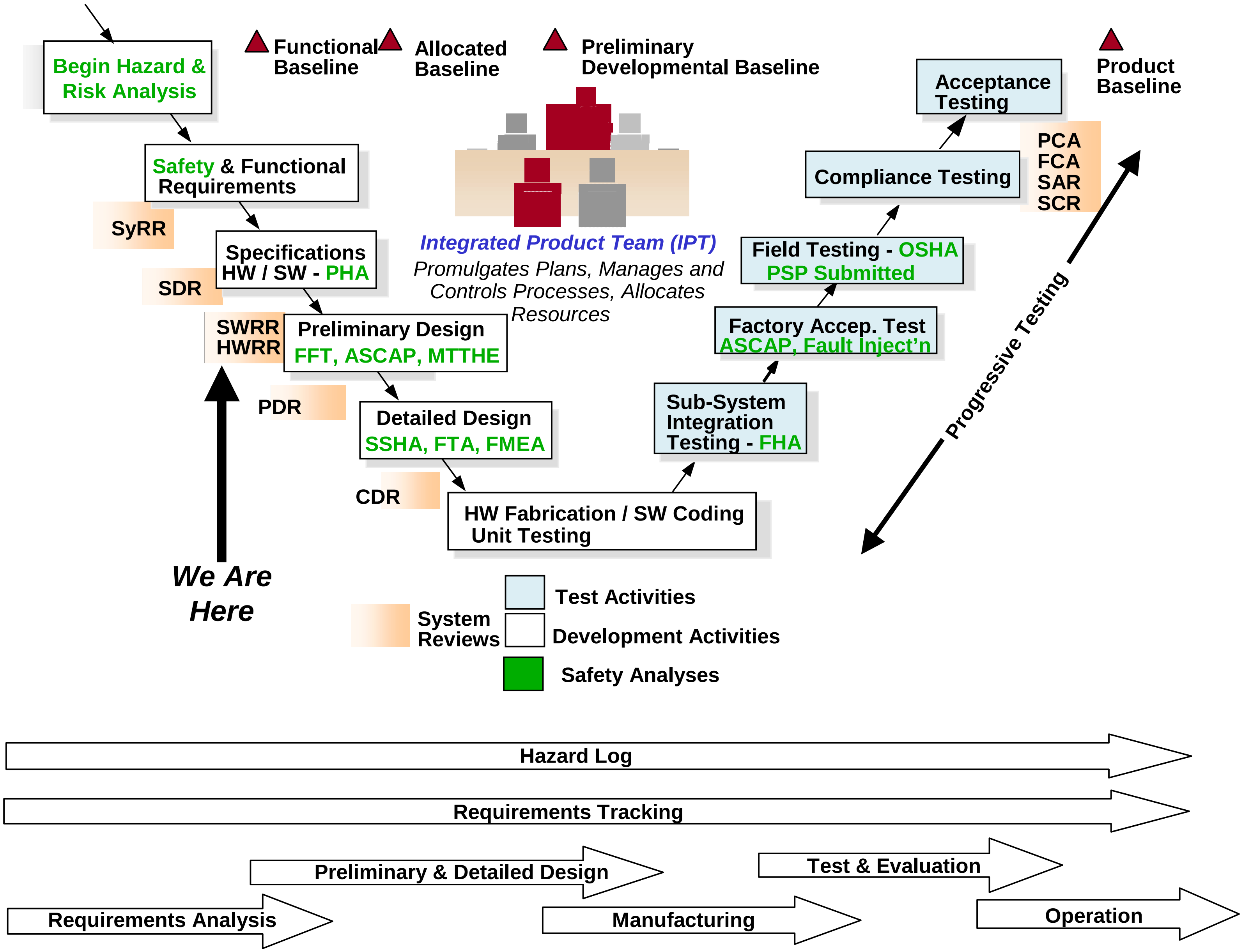
System Requirements (Continued)

- **No numeric acceptance value for Safety is specified**
  - **RSAC Draft Rule #8 specifies that PTC will not result in a risk that exceeds the existing system**
  - **Overall Safety Requirements In System Spec V3.1 include:**
    - Paragraph 4.11.1.c, SSR508: The IDOT PTC system shall incorporate a total system safety approach, rather than relying only on fail-safety of individual system components.
    - Paragraph 4.11.1.e, SSR510: The IDOT PTC system shall comply with the requirements of a Product Safety Plan (PSP) as defined in the RSPP and the draft rule developed by RSAC.
    - Paragraph 4.11.1.g, SSR512: The IDOT PTC system design shall incorporate a safety approach and safety assurance process that establishes closed-loop safety design principles.
    - Paragraph 4.11.2.b, SSR524: Safety critical functions shall be understood to mean those functions that could result in a physical conflict or other operational hazard of similar magnitude if an unsafe failure (including design error) occurs.
    - Paragraph 4.11.2.c, SSR525: Safety critical elements shall be understood to mean those elements related to the organization, issuance, safe execution, and enforcement of movement authorities.

Safety Critical System Development

- **Safety Program parallels the system development effort (Figure 1)**
- **Safety analyses are scheduled to support design effort**
    - **Key hazard analyses and UVA simulations coincide with major design reviews**
    - **Derived requirements from hazard analyses will be added to Hardware Requirements Specification (HRS), Software Requirements Specification (SRS) and requirements tracking database**
- **Derived requirements from Safety analyses incorporated into Requisite Pro database**
    - **Safety critical requirements tracked from early design through testing**
- **Contract Data Requirement List items (CDRL's) developed during course of the program (see Formal Documentation) form part of the PSP**
- **Safety is designed in on a system level**
    - **Closed loop design principles (e.g. request, grant, acknowledge)**

Figure 1 - Safety Critical System Development



Begin Hazard & Risk Analysis

Functional Baseline

Allocated Baseline

Preliminary Developmental Baseline

Product Baseline

Safety & Functional Requirements

SyRR

Specifications HW / SW - PHA

SDR

SWRR HWRR

Preliminary Design FFT, ASCAP, MTTHE

PDR

Detailed Design SSHA, FTA, FMEA

CDR

HW Fabrication / SW Coding Unit Testing

Sub-System Integration Testing - FHA

Factory Accep. Test ASCAP, Fault Inject'n

Field Testing - OSHA PSP Submitted

Compliance Testing

Acceptance Testing

PCA FCA SAR SCR

Progressive Testing

Integrated Product Team (IPT)

Promulgates Plans, Manages and Controls Processes, Allocates Resources

We Are Here

System Reviews

Test Activities

Development Activities

🟩 Safety Analyses

Hazard Log

Requirements Tracking

Preliminary & Detailed Design

Test & Evaluation

Requirements Analysis

Manufacturing

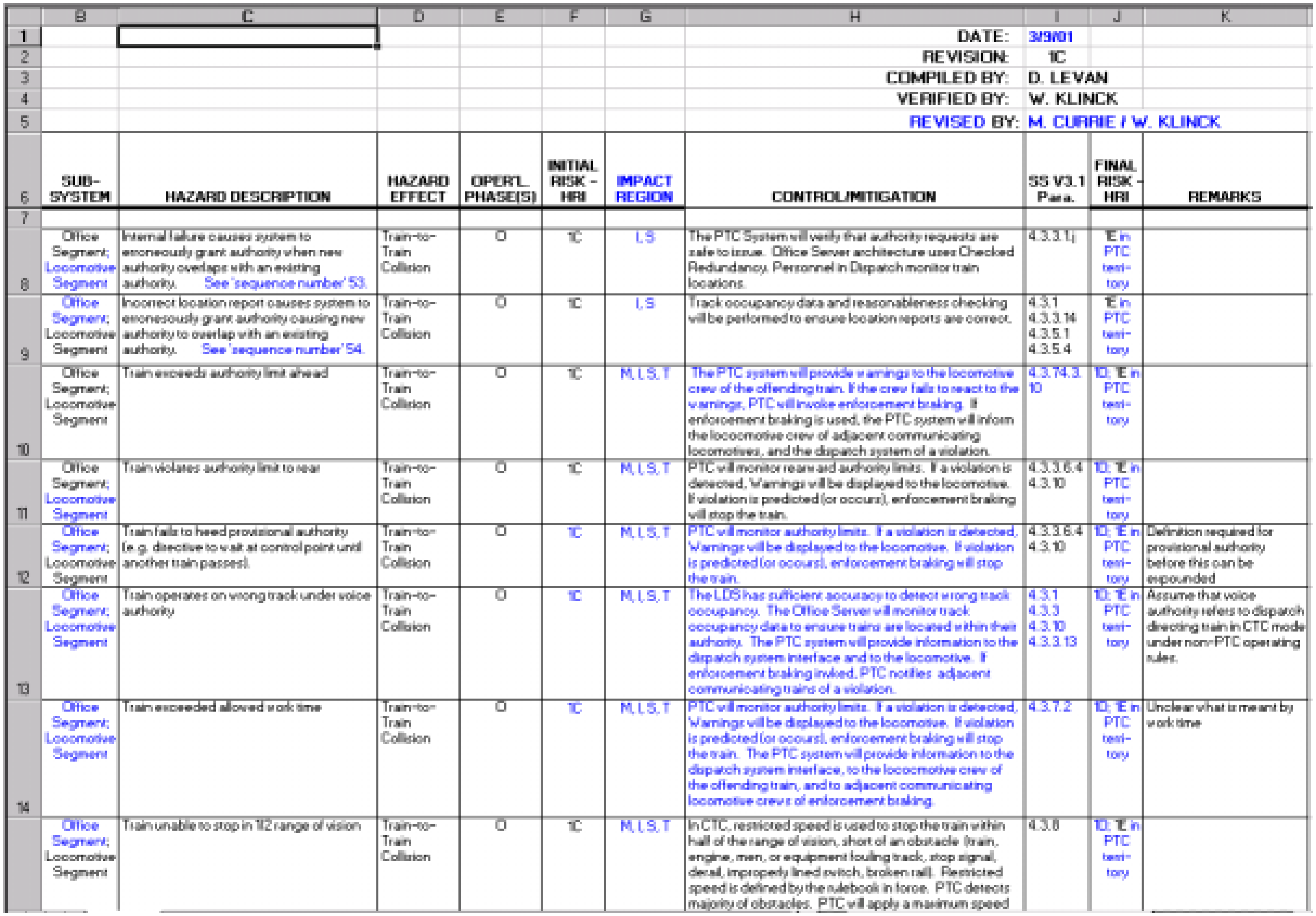
Operation

Hazard And Risk Analyses

- **Hazard analyses to be performed: PHA, FFT, SSHA, FTA, FMEA, FHA and O&SHA**

- **Recent Activity**
  - **Preliminary Hazard Analysis (PHA) completed (see Figure 2)**
    - **Currently under second review cycle**
    - **Final comments being incorporated**
    - **Interim PHA available for customer review if desired**
  - **Functional Fault Tree (FFT) (a graphical technique to identify fault sequences leading unsafe failure) have been started**
    - **Trees Generated By LM and WABTEC**
    - **Currently combining these trees**
  - **Safety Matrix created - denotes safety critical functions (see Figure 3)**
    - **Tracking document for safety critical functions**
  - **Safety Requirements Document (SRD) generated**
    - **2nd issue out for review , will be updated to add Safety Matrix**
    - **Vital / Non-Vital rating based on safety guidelines furnished with matrix**

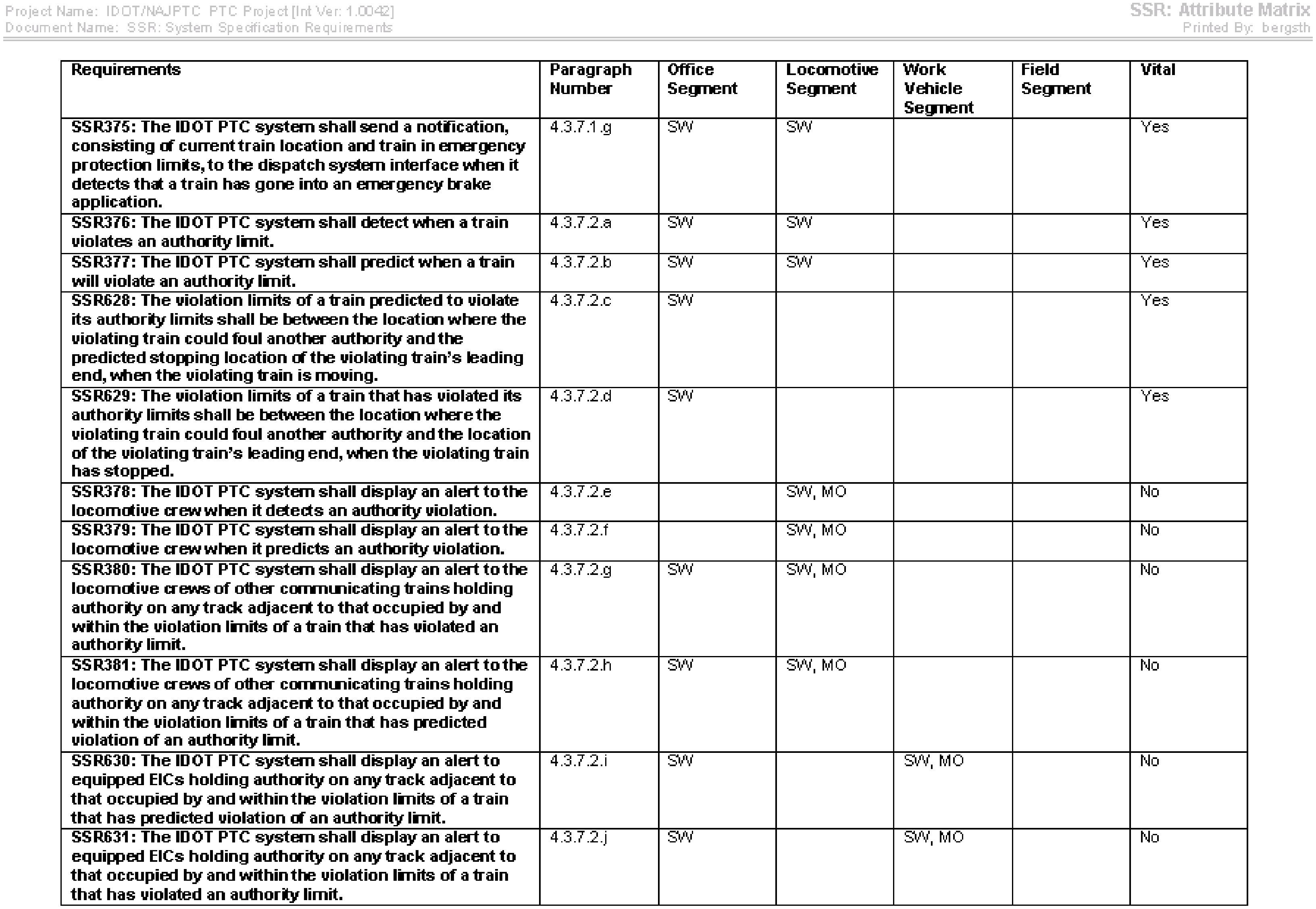
Figure 2 - Preliminary Hazard Analysis (PHA)



	B	C	D	E	F	G	H	I	J	K
1							DATE:	3/9/01		
2							REVISION:	1C		
3							COMPILED BY:	D. LEVAN		
4							VERIFIED BY:	W. KLINCK		
5							REVISED BY:	M. CURRIE / W. KLINCK		
6	SUB-SYSTEM	HAZARD DESCRIPTION	HAZARD EFFECT	OPER'L PHASE(S)	INITIAL RISK - HRI	IMPACT REGION	CONTROL/MITIGATION	SS V3.1 Para.	FINAL RISK - HRI	REMARKS
7										
8	Office Segment; Locomotive Segment	Internal failure causes system to erroneously grant authority when new authority overlaps with an existing authority. See 'sequence number' 53.	Train-to-Train Collision	O	1C	I, S	The PTC System will verify that authority requests are safe to issue. Office Server architecture uses Checked Redundancy. Personnel in Dispatch monitor train locations.	4.3.3.1.j	1E in PTC territory	
9	Office Segment; Locomotive Segment	Incorrect location report causes system to erroneously grant authority causing new authority to overlap with an existing authority. See 'sequence number' 54.	Train-to-Train Collision	O	1C	I, S	Track occupancy data and reasonableness checking will be performed to ensure location reports are correct.	4.3.1 4.3.3.14 4.3.5.1 4.3.5.4	1E in PTC territory	
10	Office Segment; Locomotive Segment	Train exceeds authority limit ahead	Train-to-Train Collision	O	1C	M, I, S, T	The PTC system will provide warnings to the locomotive crew of the offending train. If the crew fails to react to the warnings, PTC will invoke enforcement braking. If enforcement braking is used, the PTC system will inform the locomotive crew of adjacent communicating locomotives, and the dispatch system of a violation.	4.3.7 4.3.10	1D; 1E in PTC territory	
11	Office Segment; Locomotive Segment	Train violates authority limit to rear	Train-to-Train Collision	O	1C	M, I, S, T	PTC will monitor rearward authority limits. If a violation is detected, Warnings will be displayed to the locomotive. If violation is predicted (or occurs), enforcement braking will stop the train.	4.3.3.6.4 4.3.10	1D; 1E in PTC territory	
12	Office Segment; Locomotive Segment	Train fails to heed provisional authority (e.g. directive to wait at control point until another train passes).	Train-to-Train Collision	O	1C	M, I, S, T	PTC will monitor authority limits. If a violation is detected, Warnings will be displayed to the locomotive. If violation is predicted (or occurs), enforcement braking will stop the train.	4.3.3.6.4 4.3.10	1D; 1E in PTC territory	Definition required for provisional authority before this can be expounded
13	Office Segment; Locomotive Segment	Train operates on wrong track under voice authority	Train-to-Train Collision	O	1C	M, I, S, T	The LDS has sufficient accuracy to detect wrong track occupancy. The Office Server will monitor track occupancy data to ensure trains are located within their authority. The PTC system will provide information to the dispatch system interface and to the locomotive. If enforcement braking invked, PTC notifies adjacent communicating trains of a violation.	4.3.1 4.3.3 4.3.10 4.3.3.13	1D; 1E in PTC territory	Assume that voice authority refers to dispatch directing train in CTC mode under non-PTC operating rules.
14	Office Segment; Locomotive Segment	Train exceeded allowed work time	Train-to-Train Collision	O	1C	M, I, S, T	PTC will monitor authority limits. If a violation is detected, Warnings will be displayed to the locomotive. If violation is predicted (or occurs), enforcement braking will stop the train. The PTC system will provide information to the dispatch system interface, to the locomotive crew of the offending train, and to adjacent communicating locomotive crews of enforcement braking.	4.3.7.2	1D; 1E in PTC territory	Unclear what is meant by work time
	Office Segment; Locomotive Segment	Train unable to stop in 1/2 range of vision	Train-to-Train Collision	O	1C	M, I, S, T	In CTC, restricted speed is used to stop the train within half of the range of vision, short of an obstacle (train, engine, men, or equipment fouling track, stop signal, derail, improperly lined switch, broken rail). Restricted speed is defined by the rulebook in force. PTC detects majority of obstacles. PTC will apply a maximum speed	4.3.8	1D; 1E in PTC territory	

Excerpt Page (1 of 12)

FIGURE 3 - Safety Requirements Matrix



Project Name: IDOT/NAJPTC PTC Project [Int Ver: 1.0042]
Document Name: SSR: System Specification Requirements

SSR: Attribute Matrix
Printed By: bergsth

Requirements	Paragraph Number	Office Segment	Locomotive Segment	Work Vehicle Segment	Field Segment	Vital
SSR375: The IDOT PTC system shall send a notification, consisting of current train location and train in emergency protection limits, to the dispatch system interface when it detects that a train has gone into an emergency brake application.	4.3.7.1.g	SW	SW			Yes
SSR376: The IDOT PTC system shall detect when a train violates an authority limit.	4.3.7.2.a	SW	SW			Yes
SSR377: The IDOT PTC system shall predict when a train will violate an authority limit.	4.3.7.2.b	SW	SW			Yes
SSR628: The violation limits of a train predicted to violate its authority limits shall be between the location where the violating train could foul another authority and the predicted stopping location of the violating train's leading end, when the violating train is moving.	4.3.7.2.c	SW				Yes
SSR629: The violation limits of a train that has violated its authority limits shall be between the location where the violating train could foul another authority and the location of the violating train's leading end, when the violating train has stopped.	4.3.7.2.d	SW				Yes
SSR378: The IDOT PTC system shall display an alert to the locomotive crew when it detects an authority violation.	4.3.7.2.e		SW, MO			No
SSR379: The IDOT PTC system shall display an alert to the locomotive crew when it predicts an authority violation.	4.3.7.2.f		SW, MO			No
SSR380: The IDOT PTC system shall display an alert to the locomotive crews of other communicating trains holding authority on any track adjacent to that occupied by and within the violation limits of a train that has violated an authority limit.	4.3.7.2.g	SW	SW, MO			No
SSR381: The IDOT PTC system shall display an alert to the locomotive crews of other communicating trains holding authority on any track adjacent to that occupied by and within the violation limits of a train that has predicted violation of an authority limit.	4.3.7.2.h	SW	SW, MO			No
SSR630: The IDOT PTC system shall display an alert to equipped EICs holding authority on any track adjacent to that occupied by and within the violation limits of a train that has predicted violation of an authority limit.	4.3.7.2.i	SW		SW, MO		No
SSR631: The IDOT PTC system shall display an alert to equipped EICs holding authority on any track adjacent to that occupied by and within the violation limits of a train that has violated an authority limit.	4.3.7.2.j	SW		SW, MO		No

Excerpt Page (40 of 55)

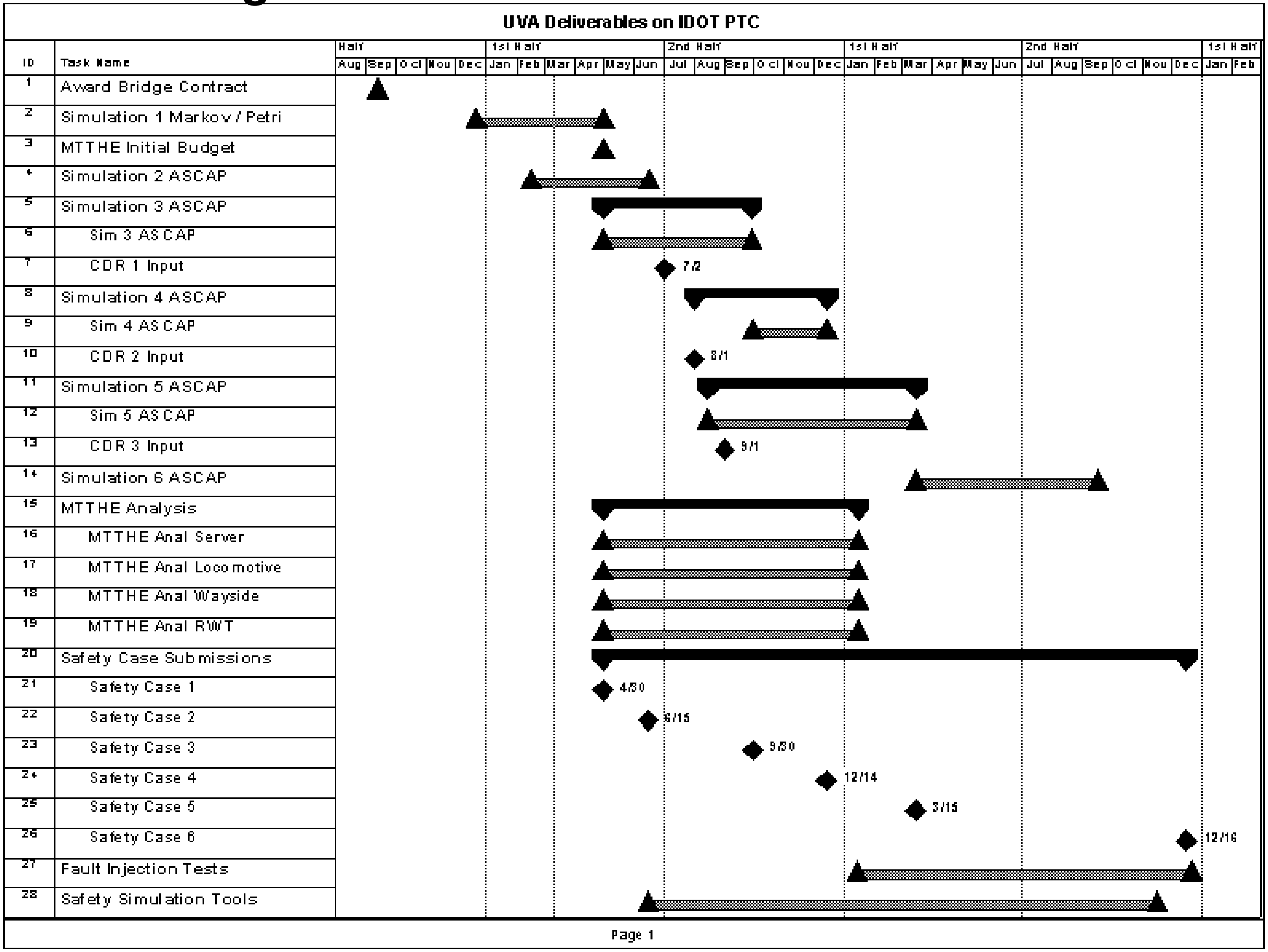
UVA Effort

- **UVA Contract Status**
  - **Under contract for full scope of program**
- **Risk Analysis will be done using Axiomatic Safety-Critical Assessment Process (ASCAP) developed by UVA**
  - **ASCAP is supported by FRA**
    - **A developing, general purpose tool for safety certifying processor based rail systems**
  - **ASCAP will be improved for use on IDOT PTC**
  - **Other rail projects analyzed using ASCAP**
    - **CSX CBTM**
    - **NYCT Canarsie Line**
    - **MAGLEV**

UVA Analysis Effort

- **ASCAP Features**
  - **Models hardware, software, operating rules, human interaction**
  - **Simulates events sequences leading to hazard**
  - **Models failure probabilities and random failures**
  - **Performs “proof of correctness” analysis**
    - **Verify system design (no faults)**
  - **Performs “proof of safety critical risk” analysis**
    - **Injects faults into system with Monte Carlo (random number) stimulation of failures**
    - **Verifies fail safe response**
- **Mean Time TO Hazardous Event (MTTHE) prediction being done by UVA**
  - **Provides “budgets” to each IDOT PTC segment**
  - **Follow on simulations and tests by UVA to confirm MTTHE budgets are met**

Figure 4 - UVA Deliverables Schedule



UVA Deliverables on IDOT PTC

ID	Task Name
1	Award Bridge Contract
2	Simulation 1 Markov / Petri
3	MTTHE Initial Budget
4	Simulation 2 ASCAP
5	Simulation 3 ASCAP
6	Sim 3 ASCAP
7	CDR 1 Input
8	Simulation 4 ASCAP
9	Sim 4 ASCAP
10	CDR 2 Input
11	Simulation 5 ASCAP
12	Sim 5 ASCAP
13	CDR 3 Input
14	Simulation 6 ASCAP
15	MTTHE Analysis
16	MTTHE Anal Server
17	MTTHE Anal Locomotive
18	MTTHE Anal Wayside
19	MTTHE Anal RWT
20	Safety Case Submissions
21	Safety Case 1
22	Safety Case 2
23	Safety Case 3
24	Safety Case 4
25	Safety Case 5
26	Safety Case 6
27	Fault Injection Tests
28	Safety Simulation Tools

Half
1st Half
2nd Half
1st Half
2nd Half
1st Half
Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb
7/2
8/1
9/1
4/30
6/15
9/30
12/14
3/15
12/16
Page 1

Safety Concepts Overview

- **Hardware approaches overview**
  - **Office Segment - Redundancy and Checking**
  - **Field Segment - Diversity and Checking**
  - **Locomotive Segment - Segment to segment cross checking; cross checking between two processors**
  - **Work Vehicle Segment (includes Roadway Worker Terminal - RWT) - Segment to segment cross checking; Closed Loop Confirmation and acknowledgement of all transmitted data**
- **Segment to segment communications uses ATCS 200 system**
  - **Provides for transmitting vital messages with Cyclic Redundancy Checks (CRC's)**

Safety Concepts Overview (Continued)

- **System approach to software fault tolerance and detection:**
  - **Reasonableness tests to verify plausibility of data**
  - **Software watchdog timers to detect processing faults**
  - **I/O done using “closed loop” request / acknowledge process**
  - **Voting / cross checking (detect faults in parallel processors)**
  - **Automatically redistribute processing functions after fault**
  - **Data hiding / encapsulation (object orientation)**
  - **Recovery blocks to re-start processing after fault**

Safety Concepts Overview (Continued)

- LM proceeding with language subsets for safety
  - Subsets avoid ambiguous features, failure-prone constructs and programmer misunderstanding
  - LM is implementing the MISRA C Subset
- Static code analyzer tools screen source code prior to compilation
  - Oakwood tool being implemented by LM
  - Analyzer finds violations of language subsets and other rules
  - LM will also use other tools, presently in use, which
    - Identify uninitialized variables, type mismatches, unused variables, memory leaks, variables with ambiguous scope
- LM using progressive testing methods:
  - Part of system safety / development process
  - Testing performed from “bottom up” to detect and remove errors as early as possible in development cycle

Formal Documentation

- **Detailed specifications form a part of the PSP describing system, hardware, software and interfaces**
  - **System Level**
    - **System Segment Design Document (SSDD)**
    - **Requirements Allocation Matrix (RAM)**
    - **Contractor Master Test Plan (CMTP)**
  - **Hardware**
    - **Hardware Development and Integration Plan (HDIP)**
    - **Hardware Requirements Specification (HRS)**
    - **Hardware Design Document (HDD)**
  - **Software**
    - **Software Development Plan (SDP)**
    - **Software Requirements Specification (SRS)**
    - **Software Design Document (SWDD)**

Formal Documentation (Continued)

- **Detailed specifications (Continued)**
  - **Interfaces**
    - **Interface Requirements Specification (IRS)**
    - **Interface Design Document (IDD)**
- **Requirements verification**
  - **Requisite Pro being used to track, allocate and verify / test requirements throughout the program**
  - **Requisite Pro database includes a field to designate the requirement as Vital (or not)**

Verification, Validation And Testing

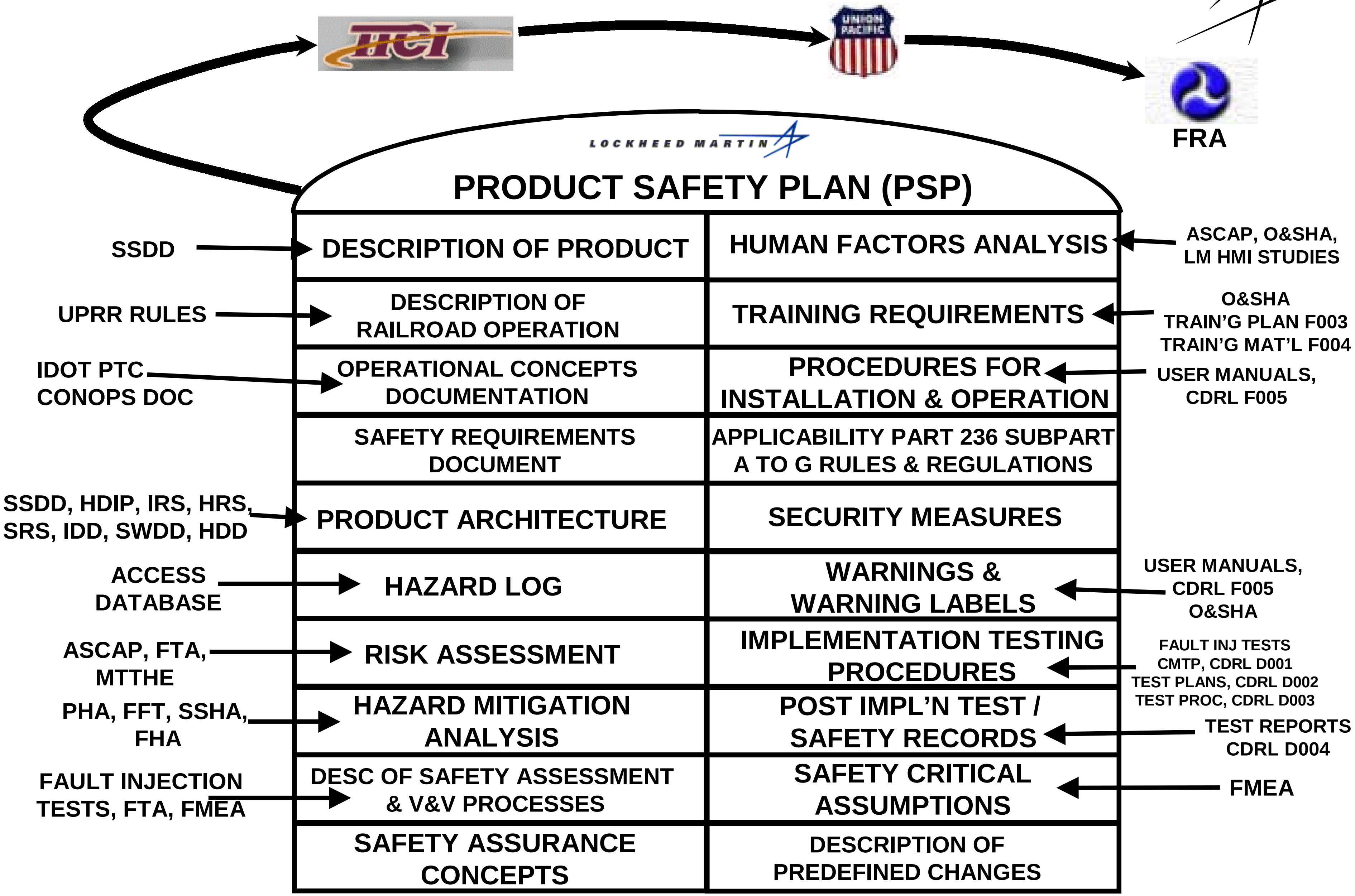
- **IDOT PTC RSPP Attachment B defines**
  - **Verification**
    - **Confirms the design meets the specs**
  - **Validation**
    - **Verifies that the specification is correct and complete**
    - **V3.1 Spec update has clarified requirements**
- **Testing method**
  - **Progressive testing - “bottom up” method**
  - **Requirements flowed down to test procedures**

Per ARP4761, Guidelines And Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment:

•Validation: The determination that the requirements for a product are sufficiently correct and complete.

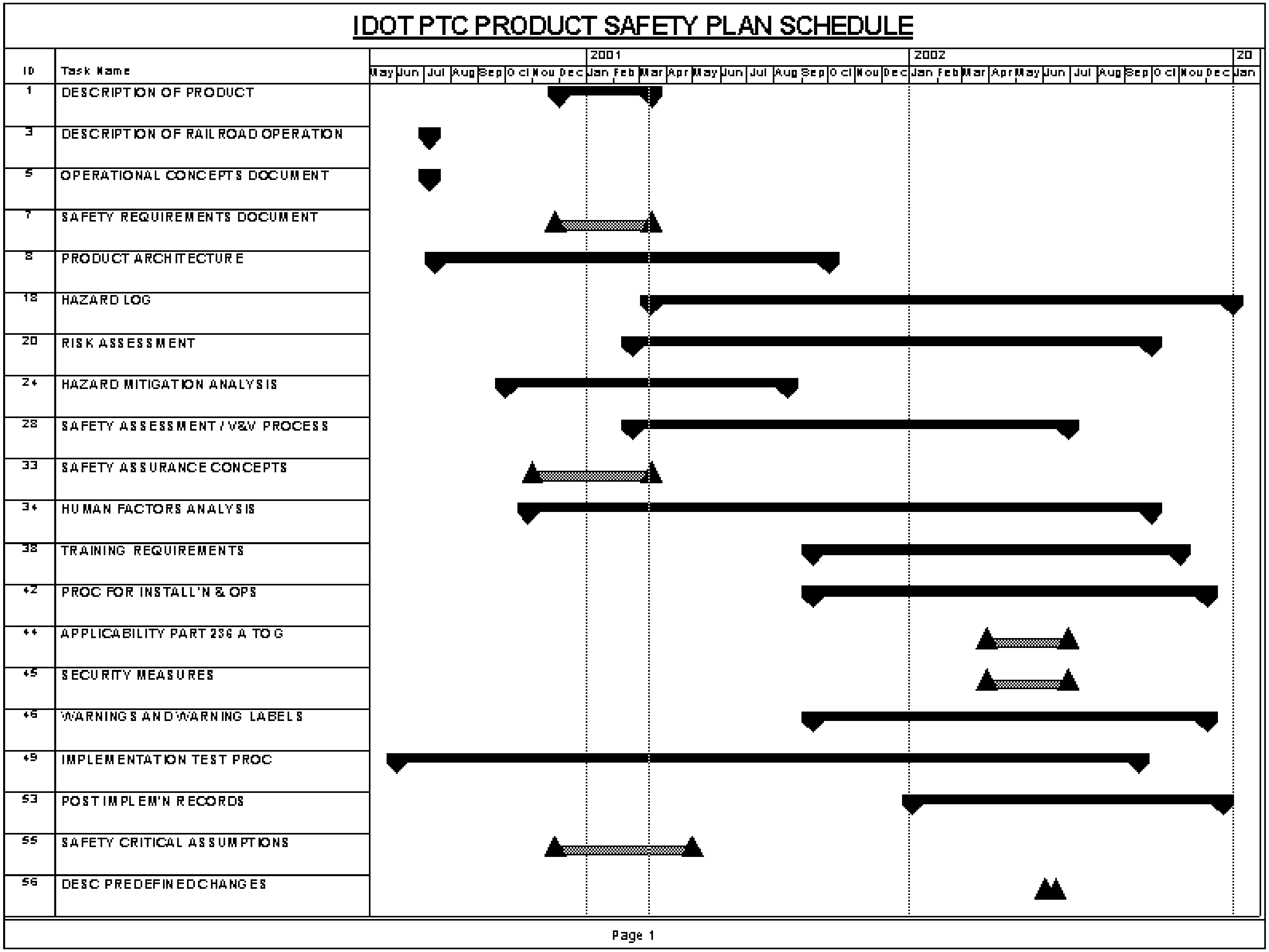
•Verification: The evaluation of an implementation to determine that applicable requirements are met.

IDOT PTC Product Safety Plan (PSP)



PRODUCT SAFETY PLAN (PSP)

SSDD	DESCRIPTION OF PRODUCT	HUMAN FACTORS ANALYSIS	ASCAP, O&SHA, LM HMI STUDIES
UPRR RULES	DESCRIPTION OF RAILROAD OPERATION	TRAINING REQUIREMENTS	O&SHA TRAIN’G PLAN F003 TRAIN’G MAT’L F004
IDOT PTC CONOPS DOC	OPERATIONAL CONCEPTS DOCUMENTATION	PROCEDURES FOR INSTALLATION & OPERATION	USER MANUALS, CDRL F005
	SAFETY REQUIREMENTS DOCUMENT	APPLICABILITY PART 236 SUBPART A TO G RULES & REGULATIONS	
SSDD, HDIP, IRS, HRS, SRS, IDD, SWDD, HDD	PRODUCT ARCHITECTURE	SECURITY MEASURES	
ACCESS DATABASE	HAZARD LOG	WARNINGS & WARNING LABELS	USER MANUALS, CDRL F005 O&SHA
ASCAP, FTA, MTTHE	RISK ASSESSMENT	IMPLEMENTATION TESTING PROCEDURES	FAULT INJ TESTS CMTP, CDRL D001 TEST PLANS, CDRL D002 TEST PROC, CDRL D003
PHA, FFT, SSHA, FHA	HAZARD MITIGATION ANALYSIS	POST IMPL’N TEST / SAFETY RECORDS	TEST REPORTS CDRL D004
FAULT INJECTION TESTS, FTA, FMEA	DESC OF SAFETY ASSESSMENT & V&V PROCESSES	SAFETY CRITICAL ASSUMPTIONS	FMEA
	SAFETY ASSURANCE CONCEPTS	DESCRIPTION OF PREDEFINED CHANGES	



IDOT PTC PRODUCT SAFETY PLAN SCHEDULE

ID	Task Name
1	DESCRIPTION OF PRODUCT
3	DESCRIPTION OF RAILROAD OPERATION
5	OPERATIONAL CONCEPTS DOCUMENT
7	SAFETY REQUIREMENTS DOCUMENT
8	PRODUCT ARCHITECTURE
18	HAZARD LOG
20	RISK ASSESSMENT
24	HAZARD MITIGATION ANALYSIS
28	SAFETY ASSESSMENT / V&V PROCESS
33	SAFETY ASSURANCE CONCEPTS
34	HUMAN FACTORS ANALYSIS
38	TRAINING REQUIREMENTS
42	PROC FOR INSTALL'N & OPS
44	APPLICABILITY PART 236 A TO G
45	SECURITY MEASURES
46	WARNINGS AND WARNING LABELS
49	IMPLEMENTATION TEST PROC
53	POST IMPLEM'N RECORDS
55	SAFETY CRITICAL ASSUMPTIONS
56	DESC PREDEFINED CHANGES

2001
2002
20
May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan

Page 1

Approval

- **Formal PSP is submitted to FRA by TTCI / UPRR**
  - **LM generated PSP provides input and detailed analyses**
  - **Initial PSP submission date is June 2002**
- **Compliance Testing and Acceptance Testing will be performed after this initial submittal**
  - **An PSP Addendum will be submitted in December 2002 providing safety related test reports from Compliance Testing and Acceptance Testing**
  - **Incremental disclosure of PSP contents will be forwarded to TTCI by LM throughout the program**
    - **CDRL's to the System Engineer (SE)**
    - **Safety Analyses**

Near Term Action

- Incorporate final comments in PHA and submit
- Complete development of Functional Fault Trees and submit
- Convene a Safety Workshop meeting with LM, Wabtec and UVA
- Initiate the Hazard Log using the PHA as a basis
- Provide information to UVA to support ASCAP model development
- Obtain additional information regarding Office Server